Ncontracts 2025 Third-Party Risk Management Survey

Trends & Insights for Financial Institutions

NCONTRACTS

ncontracts.com | 888.370.5552

Table of Contents

Executive Summary

Financial institutions are facing growing vendor risk challenges, from managing hundreds of third parties with lean teams to keeping up with evolving cybersecurity and AI risks.

Those are just a few of the findings of **The Ncontracts 2025 Third-Party Risk Management Survey**, which breaks down the biggest trends, risks, and strategies shaping third-party risk management (TPRM) at financial institutions today. Packed with real-world insights, it's your go-to resource for understanding where banks, credit unions, and mortgage companies stand — and how your institution compares.

Conducted between November 2024 and January 2025, the survey leveraged email, social media, and the Third Party ThinkTank community to reach banks, credit unions, and mortgage companies across a range of asset sizes. Responses were anonymous.

Highlights

Most FIs Are Running Lean

73% of institutions have two or fewer full-time employees managing vendor risk, even though more than half oversee 300+ vendors.

Regulatory Pressure is High

Two-thirds of institutions feel pressure to enhance TPRM programs, with auditors and regulators often pushing for improvements.

Cyber and AI Risks Are Top Concerns

Nearly half of institutions experienced a third-party cyber event last year, and AI ranks as the second-biggest TPRM risk heading into 2025.

Due Diligence Remains a Challenge

Collecting and analyzing vendor documents is a top bottleneck.

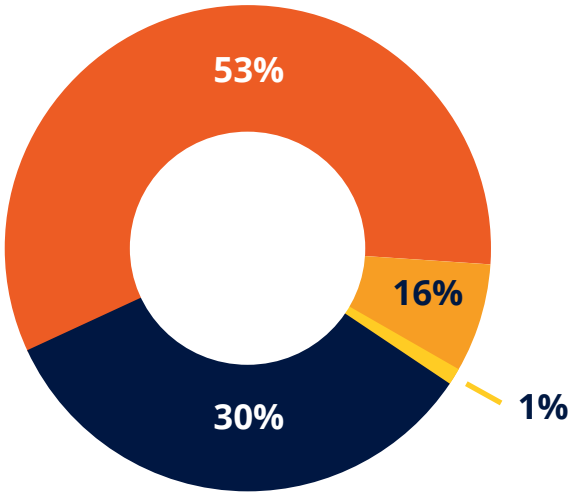
Most FIs See Strong ROI in TPRM

85% of financial institutions see moderate to high value from their TPRM programs, benefitting from improved cybersecurity, cost savings, and stronger vendor oversight.

About the Respondents

What is your asset size?

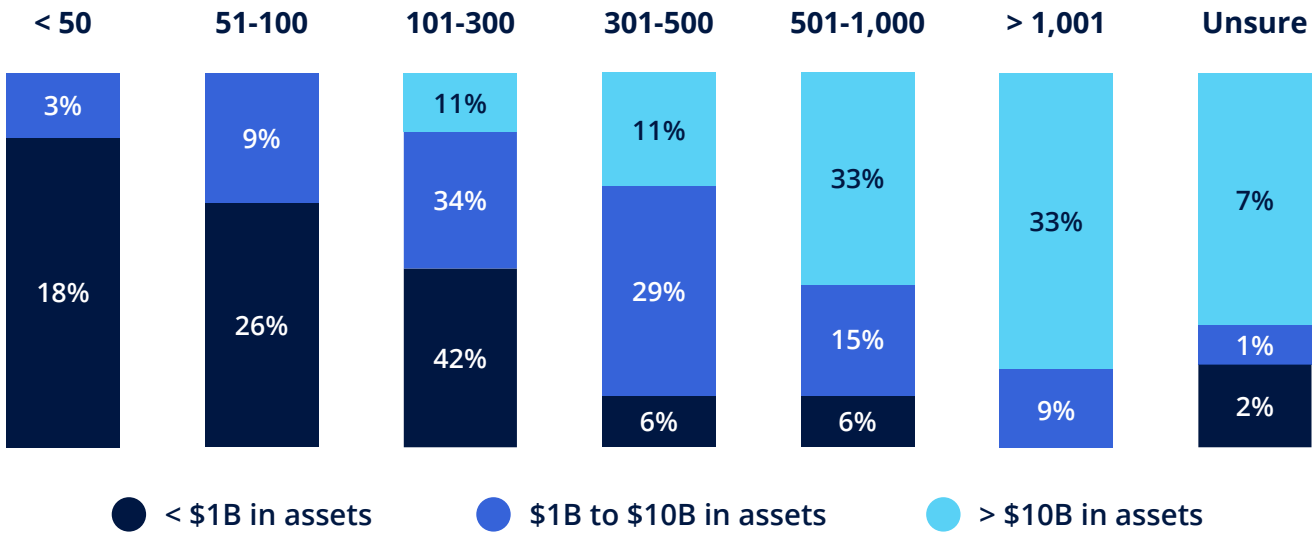
- < 1B$
- $1B to $10B
- > $10B
- N/A



TPRM Programs at Financial Institutions

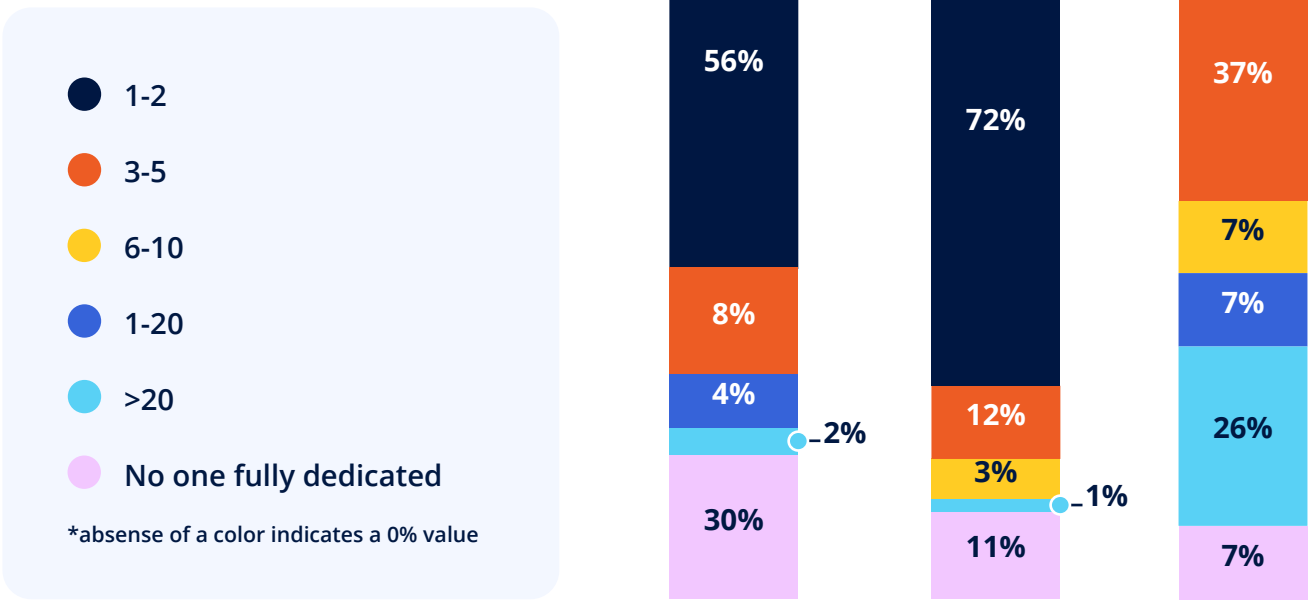
Financial institutions manage literally hundreds of vendor relationships — and the larger the institution, the larger the vendor portfolio. Among institutions with less than $1 billion in assets, 42% manage between 101 and 300 vendors — and another 12% manage between 301 and 1,000 vendors. Meanwhile, one-third of institutions with more than $10 billion in assets manage more than 500 vendors and another third manage over 1,000 vendors.

How many total vendors are included in your third-party risk management program?

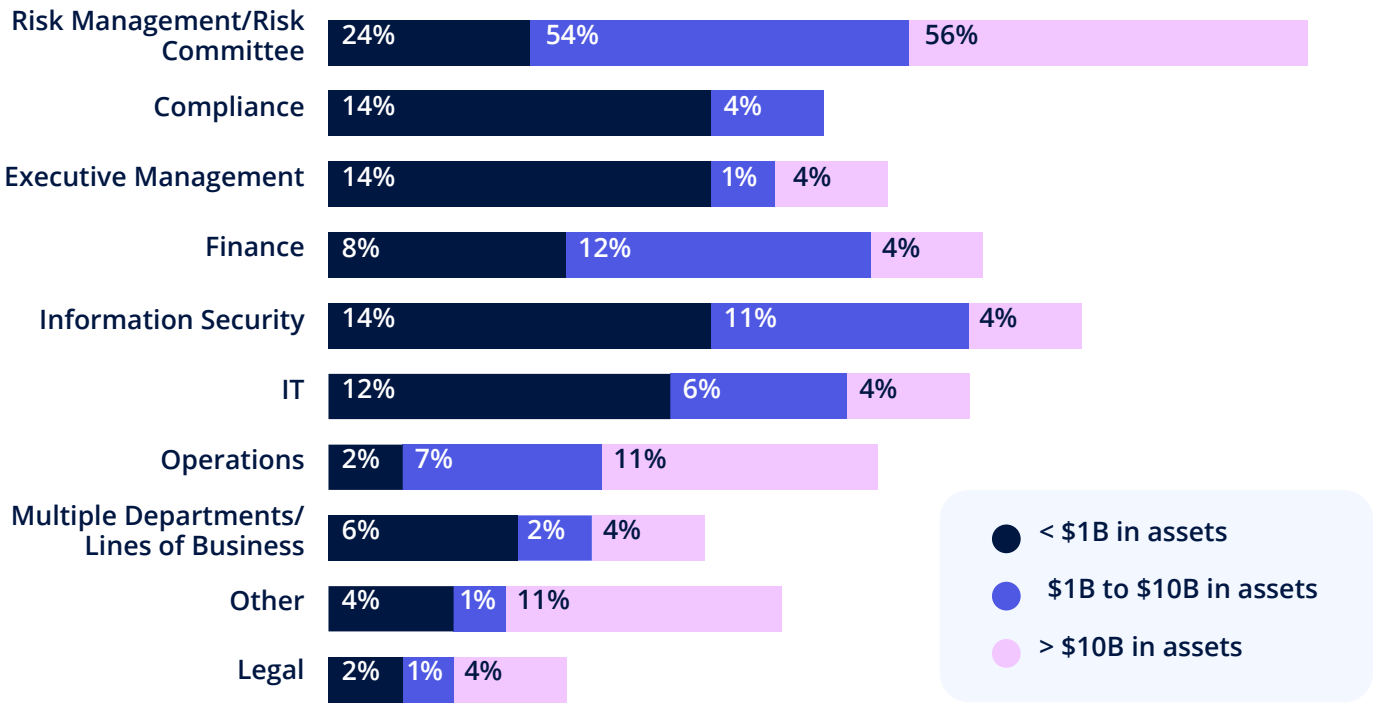


Managing a large number of vendors falls to a surprisingly small number of staff at many institutions. Outside of the largest organizations, just one or two full-time employees typically handle vendor risk management. In some cases, there are no full-time employees dedicated to TPRM.

How many full-time employees are dedicated to your third-party vendor management program?



Which department does third-party risk management report to?



Governance is a cornerstone of third-party risk management, and where TPRM reports matters. At larger financial institutions, TPRM is most likely to sit under risk management or a risk committee — 56% of institutions with over $10 billion in assets place it there, compared to just 24% of those under $1 billion in assets. This reflects a shift toward viewing TPRM as part of integrated risk management rather than a standalone compliance or IT function. Operations is also a growing home for TPRM (11% at larger institutions), highlighting its role in operational resilience and continuity planning.

"Our TPRM program was originally under our Risk Management department, but the department was overwhelmed with operational tasks and other risk-related activities, so we elected to create a separate TPRM program. It's currently under our Service department, but we still work very closely with Risk Management for certain activities."

– Bank, less than $1B in assets

What is your primary tool for managing vendor risk?

A dedicated vendor risk management software platform

Manual (spreadsheets/ databases/ SharePoint)

A vendor risk management module inside of an ERM, GRC, or other platform

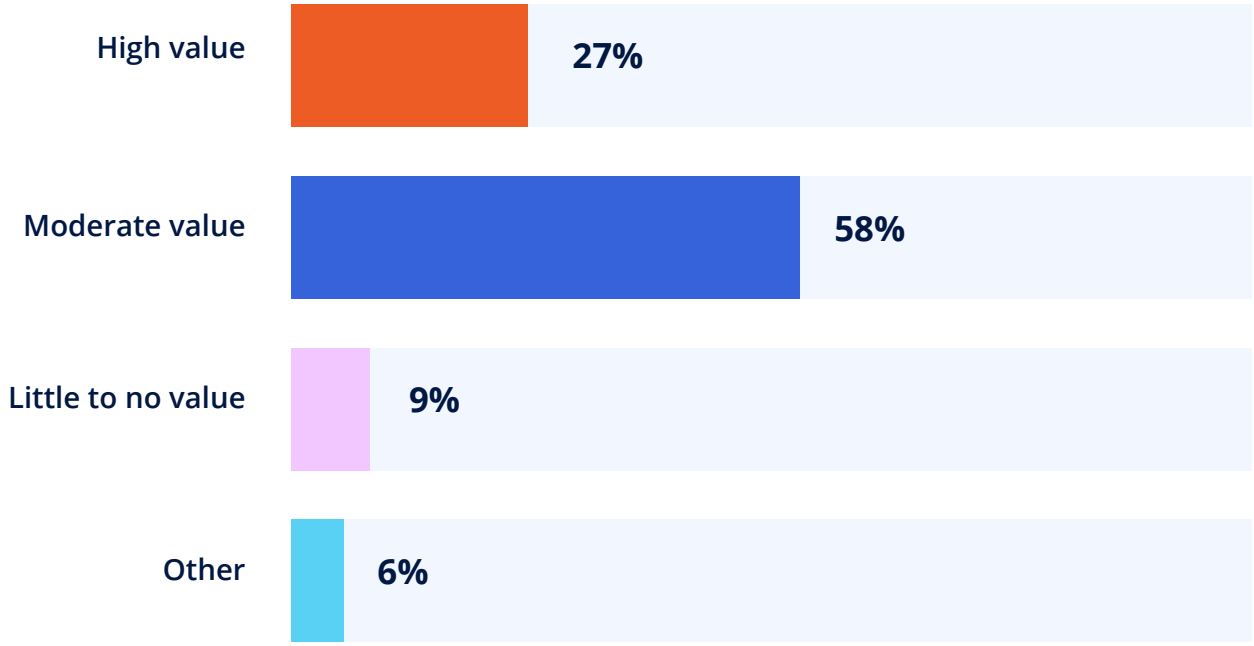
Other

Perhaps that's why so many organizations rely on TPRM software, with 85% of financial institutions using either a dedicated TPRM software platform or a module inside an enterprise risk management platform. Managing third-party risk requires tracking a vast amount of vendor data, monitoring deadlines and tasks, and ensuring ongoing vendor risk assessments across multiple departments — responsibilities that quickly become unmanageable without centralization and automation. Manual tools are most common at financial institutions with less than $1 billion in assets, where 24% report using spreadsheets, databases, or SharePoint to manage TPRM.

Organizational Approaches to TPRM

Financial institutions overwhelmingly see the value in TPRM, with 85% reporting a moderate or high return on their investment. While compliance is a key driver, institutions also recognize the broader benefits — enhancing operational resilience and cutting costs through smarter contract management. In fact, fewer than 10% view TPRM as just a regulatory obligation.

Does your organization believe there's a return on investment/value from investing in TPRM activities?



What primary benefit(s) do you believe third-party risk management gives your organization?

1. Meet regulatory requirements
2. Protect our brand and reputation
3. Avoid third-party cyber incidents
4. Align with industry best practices and standards
5. Manage vendor performance
6. Control vendor costs

The Benefits of Third-Party Risk Management

"Dedicated TPRM team decreases TPRM-related work from business and makes their daily work much easier."

Bank,
more than $10 billion in assets

"We meet FDIC vendor management requirements and make wiser decisions in selecting long-term vendor partners and products that align with our company values."

Bank,
$1 to $10 billion in assets

"3rd party incidents are now the most common problem with credit unions. Paying attention to the status and health of your 3rd party customers is essential to reduce probability of problems."

Credit Union,
less than $1 billion

"Awareness of potential risks regarding a third-party's relationship with our bank. This includes the ability to properly analyze the internal controls of the third party in order to understand the outstanding risks. This also has helped us find better third-party alternatives that had better controls and allowed us to feel more confident in working with them."

Bank,
$1 to $10 billion in assets

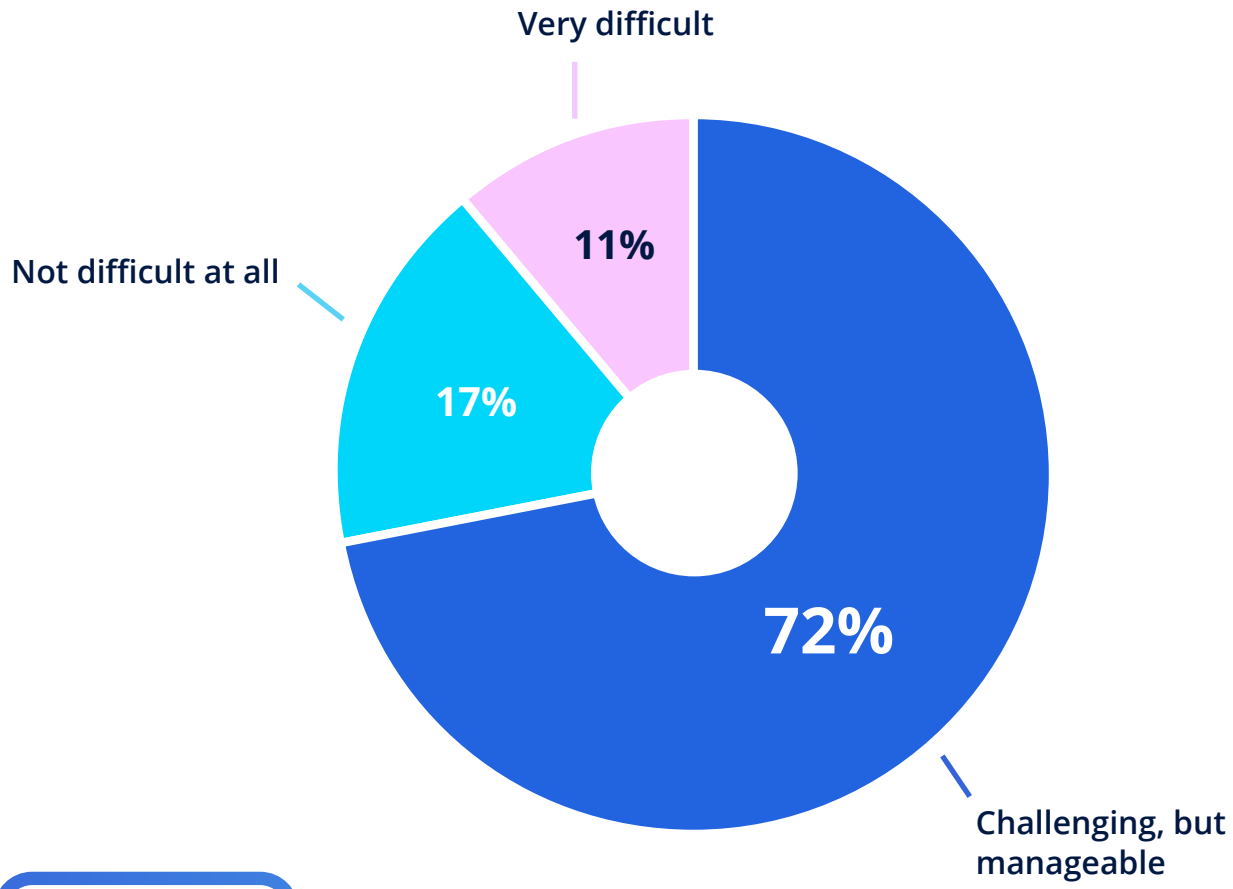
"Ensuring our vendors are compliant and provide organization for contract management."

Mortgage lender,
101-250 employees

Securing vendor owner or business unit support for TPRM isn't the easiest task, but it's manageable, according to 72% of financial institution respondents. As one institution noted, "Management sees the value when oversight provides them with supporting evidence of onboarding or exiting a vendor. Other staff within the bank see very little value as it adds to what they see as red tape for getting a vendor in place."

Other respondents remarked on TPRM's value, given increased regulatory scrutiny and the impact on their organizations. As one credit union remarked, "The better I do at uncovering/ reporting vendor concerns, the more attention TPRM gets."

How difficult is it to secure vendor owner/ business support for TPRM?



TPRM Program Maturity & Development

Financial institutions operate using one of three TPRM models:

Hybrid

Dedicated TPRM team responsible for framework, task assignment, quality control, and oversight. Vendor risk and performance management are the responsibility of vendor owners across the organization.

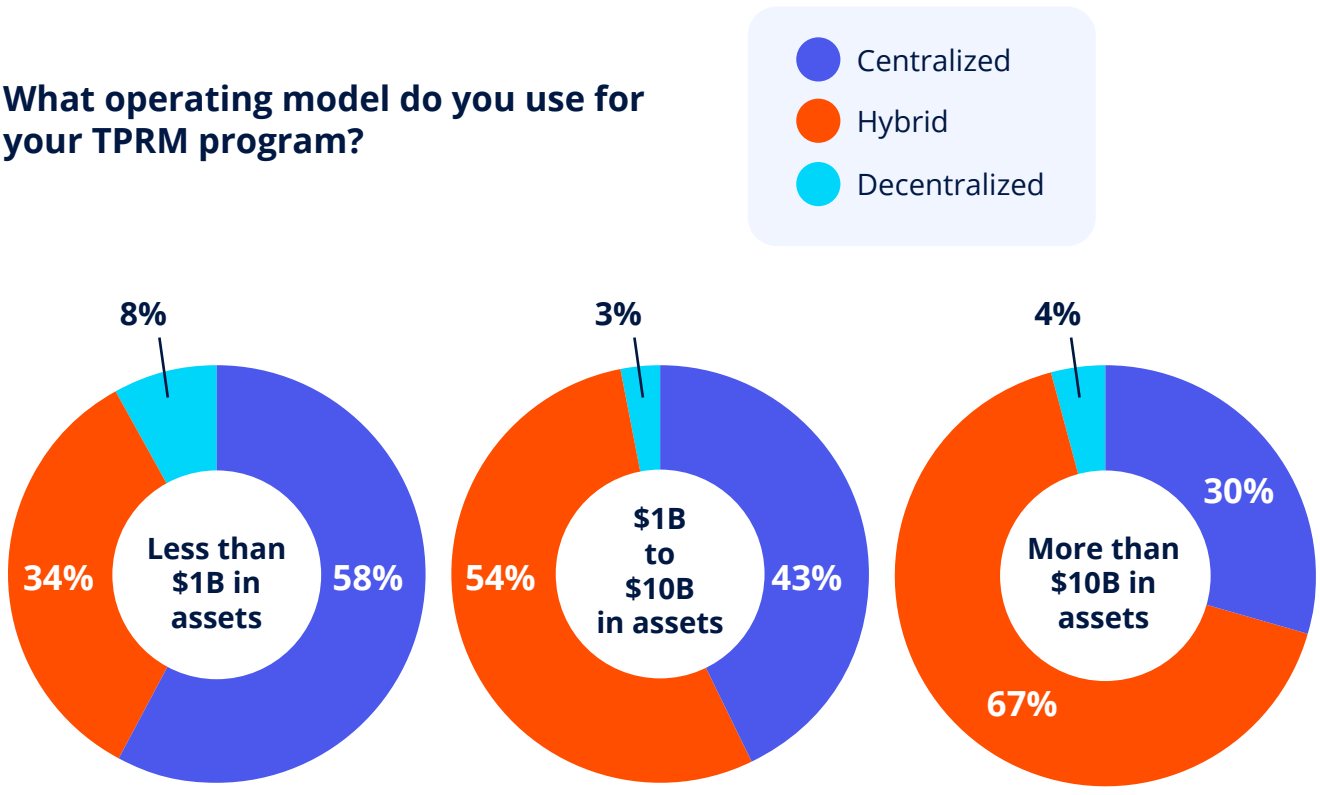
Centralized

All TPRM functions, including risk and performance management, are handled by the same team.

Decentralized

No dedicated TPRM team, responsibilities for TPRM are distributed across the organization.

What operating model do you use for your TPRM program?

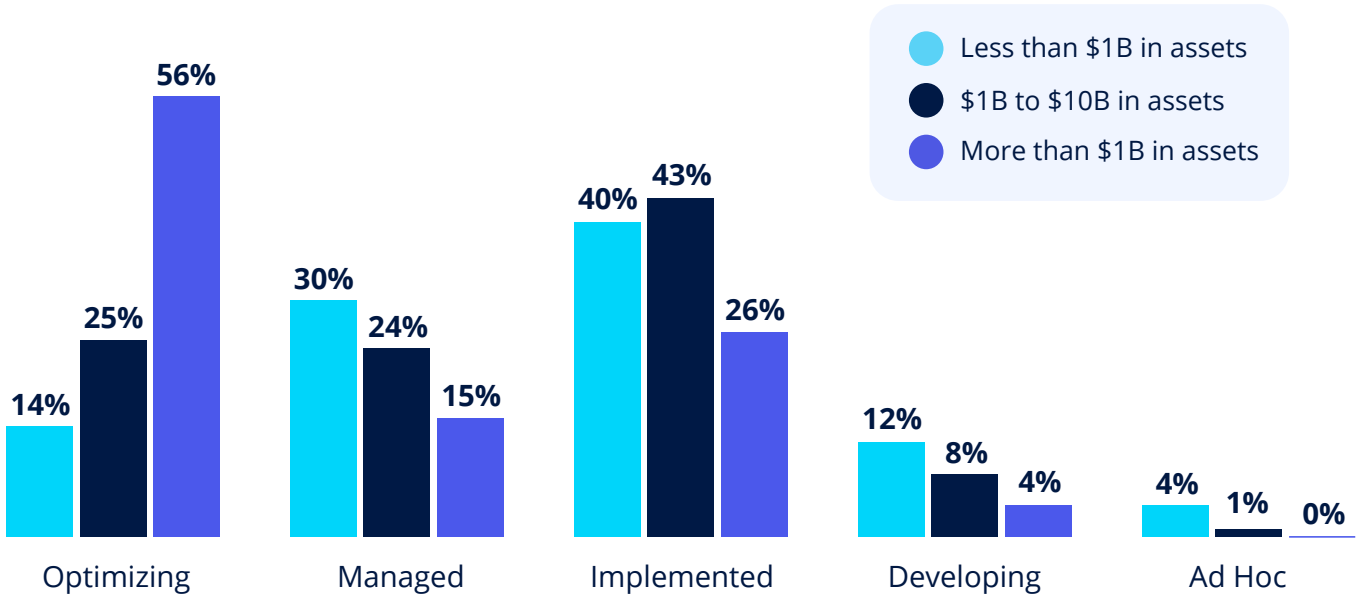


The survey shows that larger institutions favor the hybrid TPRM model, with usage increasing from 34% in banks under $1B to 67% in banks over $10B. This approach allows a dedicated TPRM team to oversee the big picture while vendor owners manage risk and performance, balancing flexibility with oversight and consistency. In contrast, smaller institutions rely more on centralization, with 58% of banks under $1 billion using a single team to handle all TPRM functions. While this ensures efficiency and control, they may struggle to scale with increasing vendor complexity.

Decentralization is rare across all asset sizes, with only 8% of small banks, 3% of mid-sized banks, and 4% of large banks taking this approach. This suggests that financial institutions recognize the risks of a fragmented TPRM process, where inconsistent oversight could create gaps in vendor risk management. The trend toward hybrid and centralized models reflects the industry's focus on structured TPRM strategies.

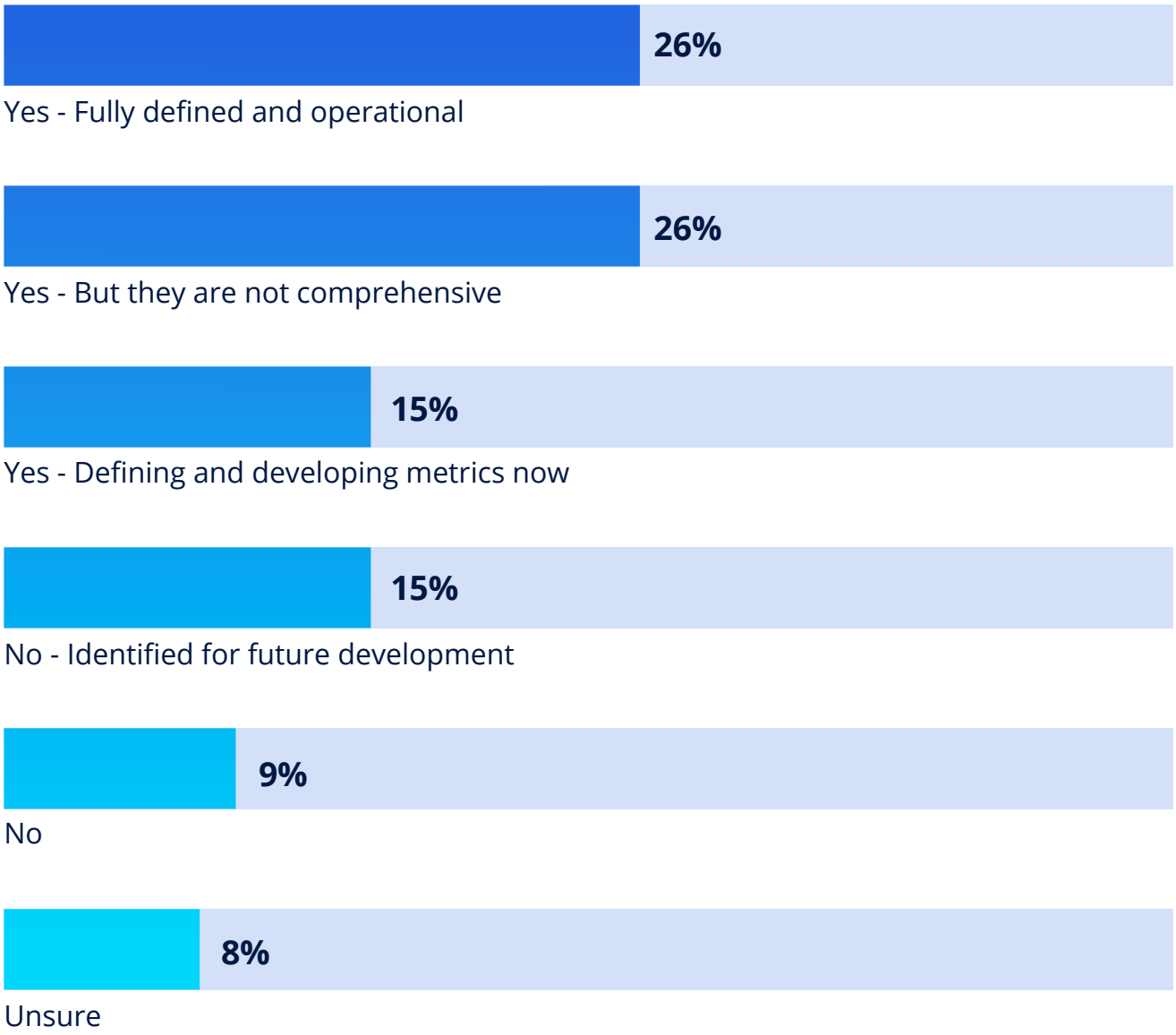
This aligns with how financial institutions view the maturity of their TPRM programs. Across all asset sizes, nearly 90% of financial institutions say their TPRM program is established, but maturity levels vary. Just over a quarter (27%) have fully integrated TPRM into their broader risk management framework, with continuous monitoring and updates. Another 23% consider their program Managed — fully established but not yet optimized — while the largest group (39%) sees their program as Implemented but in need of improvement. Smaller institutions are the least likely to have reached the Optimizing stage, with most still refining their processes.

What stage of development is your third-party risk management program in?



Similarly, large- and medium-sized banks are most likely to say their program has defined metrics to measure the health, stability, and effectiveness of their TPRM program (30%), while institutions with less than $1 billion in assets are most likely to say they have metrics in place, but they aren't comprehensive (26%). Institutions with more than $10 billion in assets are more likely to evaluate TPRM metrics than those with fewer assets. However, over a quarter (26%) of respondents, regardless of asset size, either lack metrics or are unaware of them.

Does your organization have defined metrics to measure the health, stability, and effectiveness of the third-party risk management program?



TPRM Updates and Practices

Vendor management isn't static — risk is always evolving. Financial institutions recognize this reality and are taking a proactive approach to third-party risk management (TPRM).

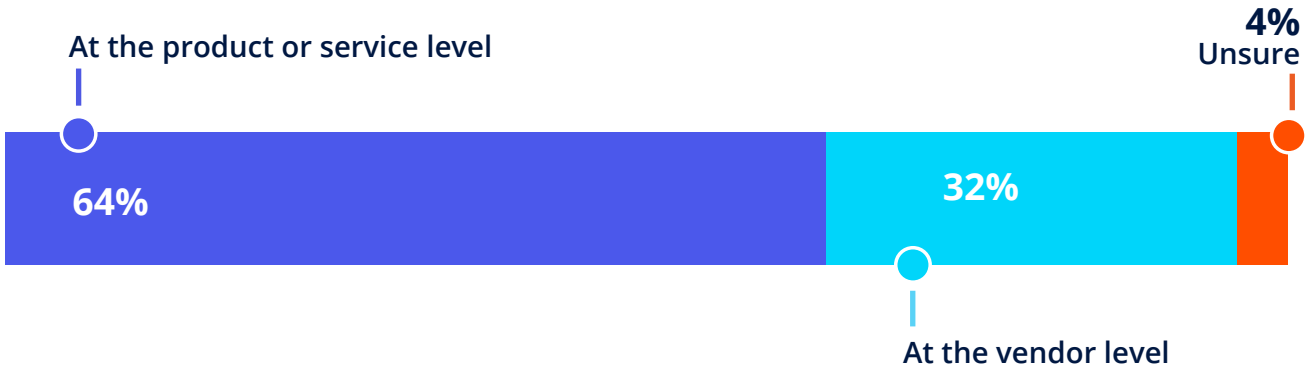
To gauge how institutions navigate vendor risk, we surveyed respondents on key TPRM activities. The results show strong alignment with best practices and regulatory expectations, reinforcing the strength of their programs and their ability to mitigate external risks.

This proactive stance is no surprise. Banks and other financial institutions operate under strict regulations, and the Interagency Guidance on Third-Party Relationships: Risk Management, released in 2023, has further emphasized the need for rigorous oversight.

For example, two-thirds (64%) of financial institutions assign vendor risk ratings at the product or service level instead of at the vendor level. This best practice ensures a more precise assessment because it recognizes that different offerings from the same vendor carry varying risk levels. For example, a core banking provider may also offer cybersecurity consulting. While a core provider is certainly a critical vendor, a consultant with no access to systems or sensitive data isn't.

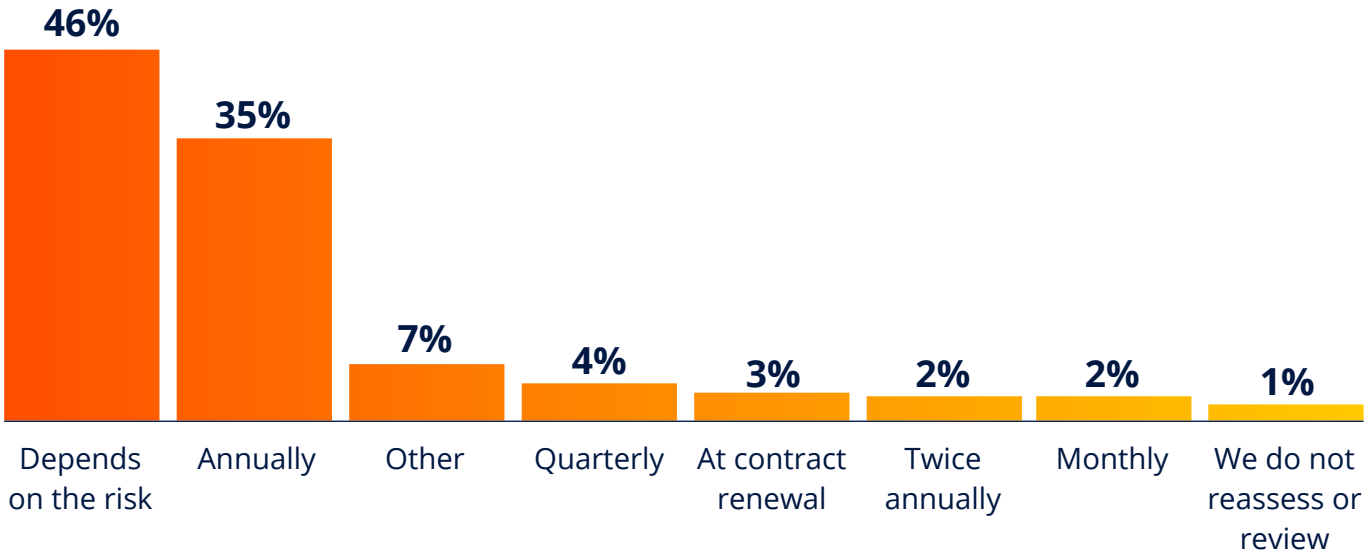
This approach aligns oversight with actual risk exposure, improving compliance, resource allocation, and risk mitigation.

How do you assign risk ratings?

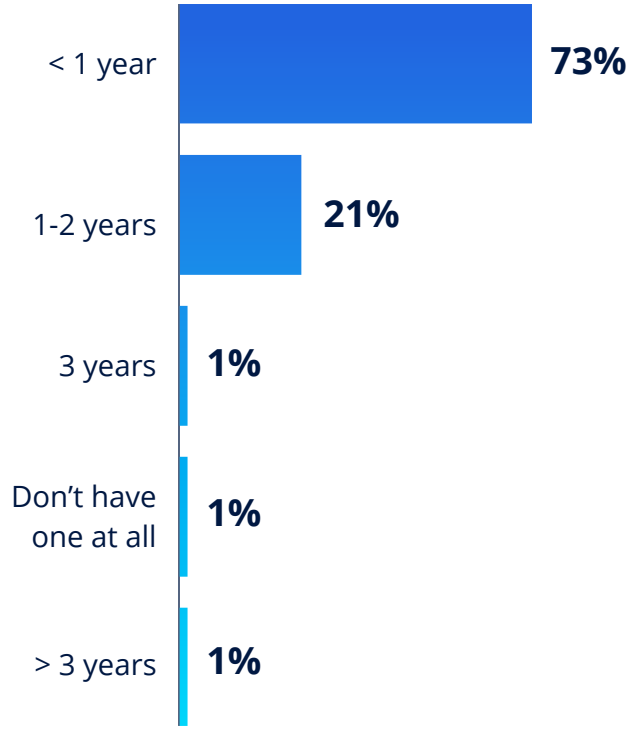


Gone are the days of static risk management — financial institutions are regularly reviewing and updating key TPRM documents to stay proactive and protect their institutions.

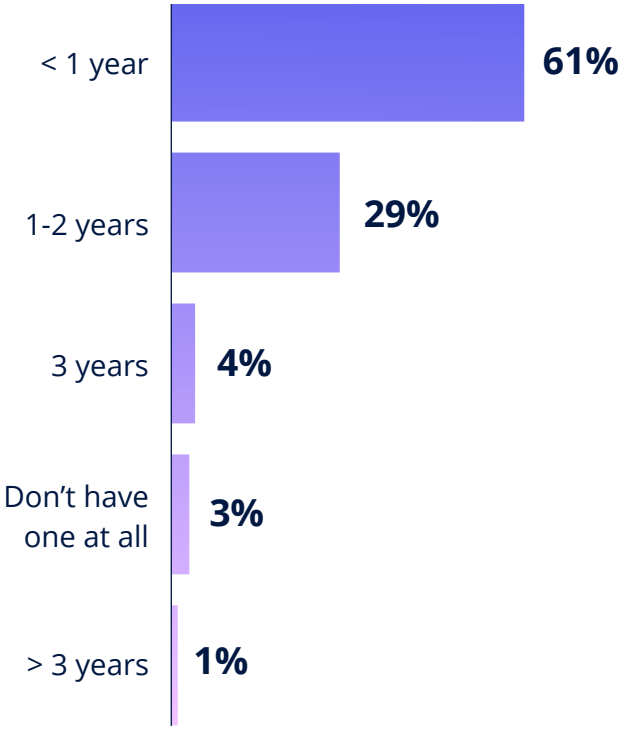
How often are you reassessing and reviewing vendor risk profiles and documentation?



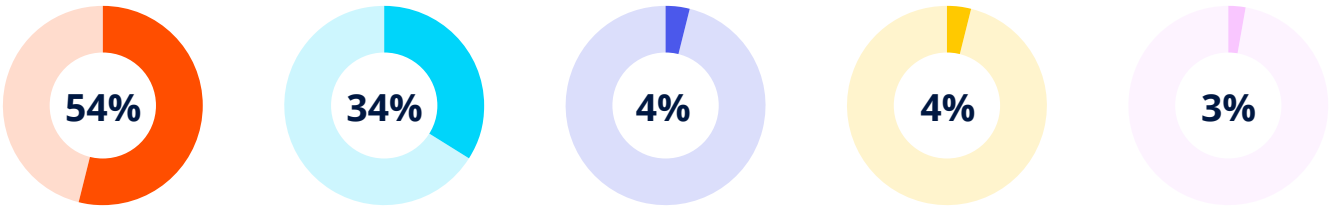
How recently have you updated your third-party risk management policy document?



How recently have you updated your inherent vendor risk assessment?



How recently have you updated your vendor risk questionnaire and due diligence document requirements?

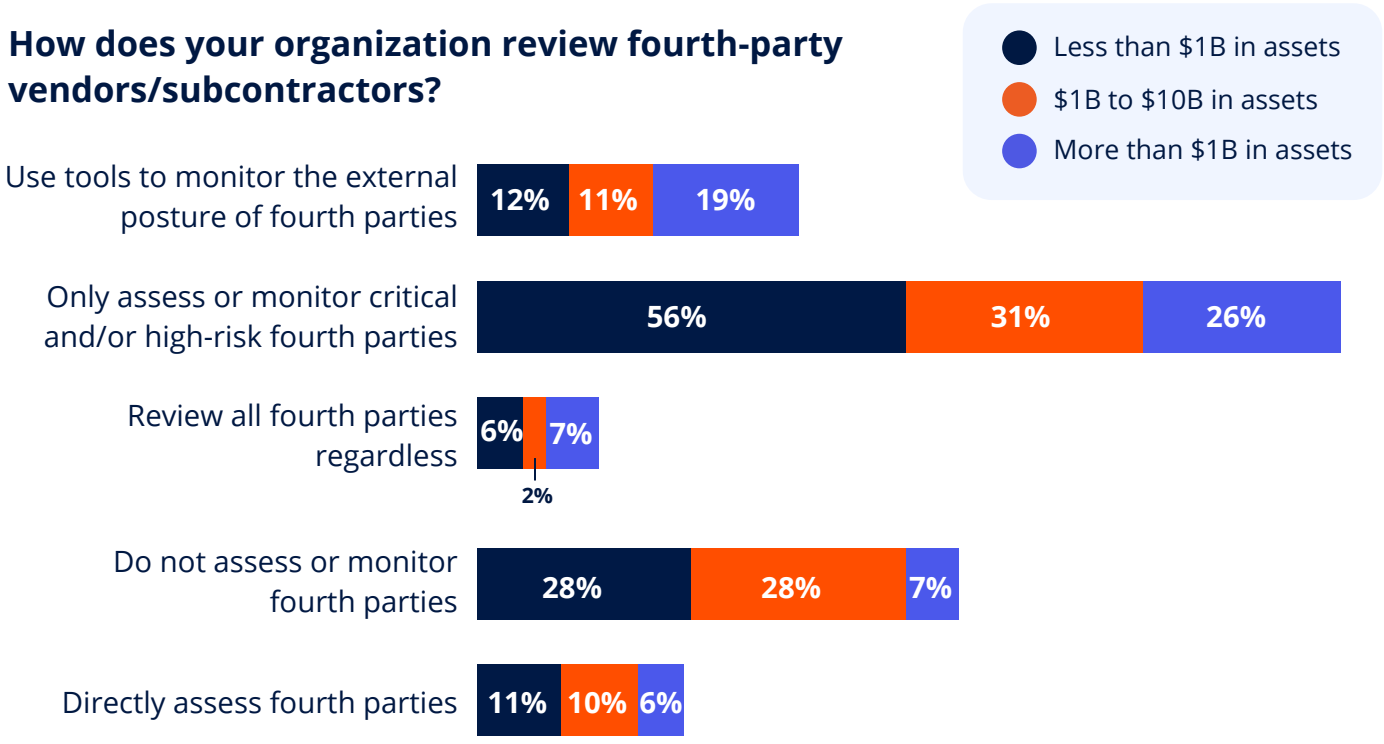


< 1 year | 1-2 years | 3 years | > 3 years | Do not have a vendor risk questionnaire or document requirements

Approaches to Fourth-Party Risk Management

For most financial institutions, fourth-party risk management isn't about direct oversight — it's about ensuring vendors have strong vendor management practices in place. The data reflects this approach, showing that institutions generally limit direct involvement while focusing on high-risk relationships and external monitoring tools where necessary.

How does your organization review fourth-party vendors/subcontractors?

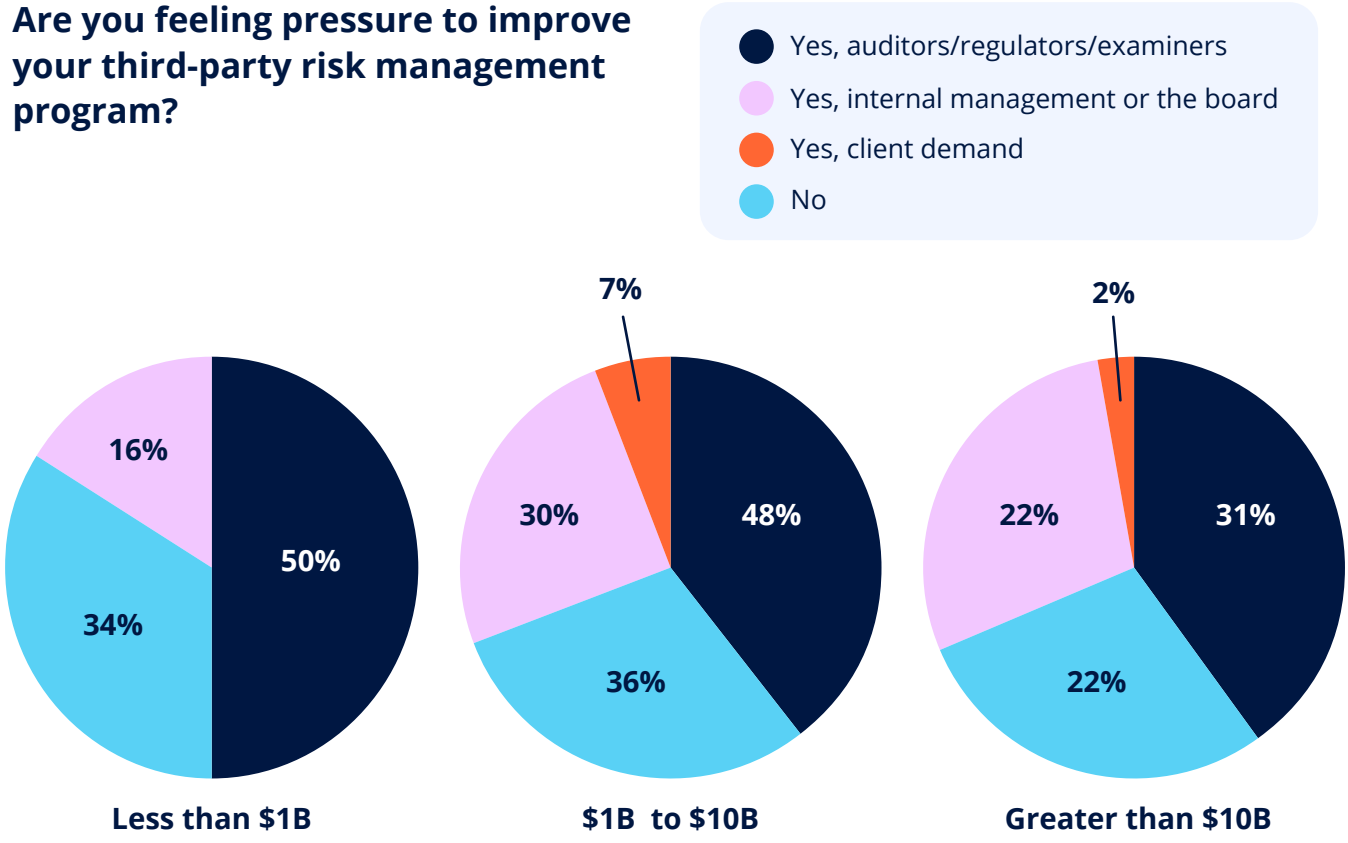


Pressure to Improve TPRM Programs

Third-party risk management (TPRM) is under pressure from all sides. Two-thirds of financial institutions (66%) report feeling pressure to enhance their TPRM programs.

Where is that pressure coming from? In many cases, regulators and auditors are the primary force behind these improvements, with nearly half of all institutions citing external oversight as a driving factor. Internal management and boards are also increasing scrutiny, particularly at mid-sized institutions, where 30% report feeling pressure from leadership. While client demand is not a major factor (0%–7%), it is emerging as a consideration for some larger institutions.

Are you feeling pressure to improve your third-party risk management program?



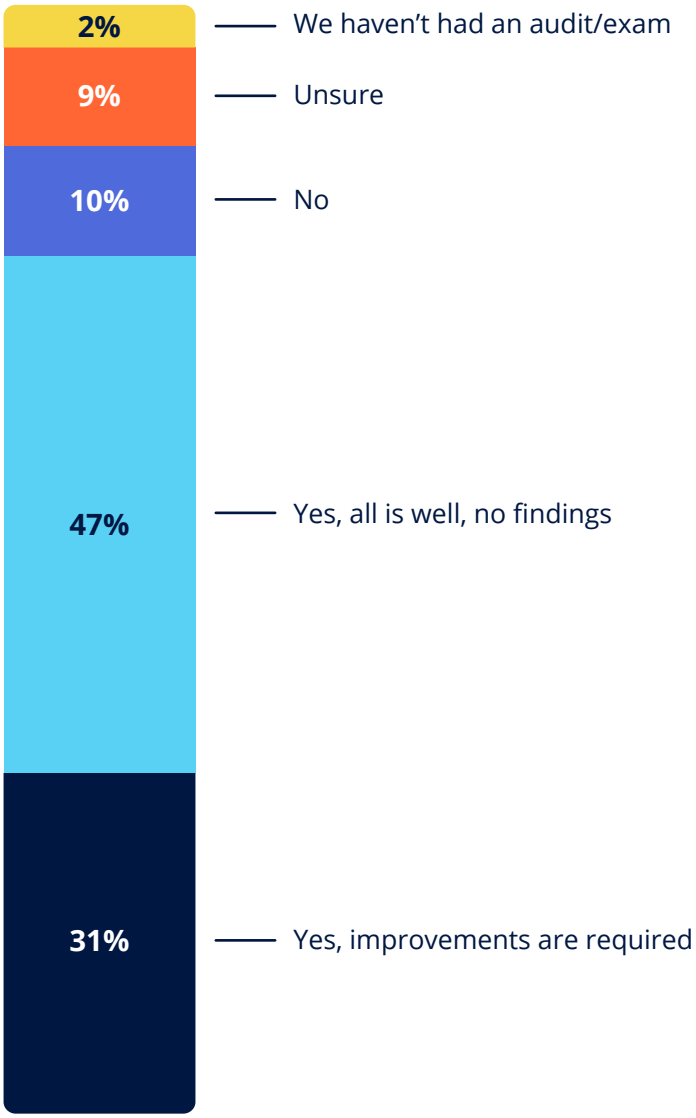
When asked about their last exam or audit, institutions across all asset sizes reported consistent results. Nearly one-third (31%) were told improvements were required, reinforcing the idea that regulators are pushing institutions to refine their TPRM programs.

A closer look at the data reveals issues are most common among those with under-developed TPRM programs. More than half (56%) of those still using manual methods like spreadsheets and Access as their primary vendor risk management tool report that they were told their TPRM program needed improvements during the last audit or exam.

Proactive TPRM makes a difference too. Respondents who reported reviewing their TPRM policy document within the last year were the most likely to say that they had no findings after an audit or exam (56%) compared to those who reviewed it in the last 1-2 years (42%).

Institutions relying on manual TPRM methods are far more likely to receive regulatory and audit findings, while those that proactively review their policies see better outcomes. Strengthening TPRM programs before an exam — not in response to one — can make a significant difference in compliance success.

During your last exam/audit, did your regulator/auditors provide feedback on your current third-party risk management program?



Emerging Risks and Challenges for 2025

As organizations prepare for 2025, third-party risk management (TPRM) remains a critical area of focus. Our survey reveals the top challenges third-party risk management professionals face and the key risks that are shaping the evolving landscape.

Top Challenges in TPRM

Organizations continue to struggle with fundamental aspects of vendor risk management, particularly around documentation, resources, and time constraints. The top challenges identified include:

- **Getting the right documents from vendors and analyzing vendor reports** (e.g., SOC reports, financials, contracts) rank among the most pressing issues, highlighting a persistent documentation bottleneck.
- **Limited internal resources and time management** hinder organizations trying to execute thorough third-party risk assessments.
- **Automation and process improvements** are priorities, with many organizations seeking to streamline vendor due diligence and risk assessment workflows.
- **Cybersecurity awareness and regulatory compliance** remain key concerns, reinforcing the need for stronger monitoring and response strategies.

Top 10 Third-Party Risk Management Challenges

1. Getting the right documents from vendors
2. Having enough internal resources
3. Time management
4. Analyzing vendor documents (e.g., SOC reports, financials, contracts)
5. Automating the process
6. Completing risk assessments
7. Tailoring our due diligence requests to be appropriate for each vendor
8. Managing contracts and negotiations
9. Awareness of our vendors' cybersecurity
10. Keeping up with the regulations

Top Third-Party Risks Heading into 2025

TPRM risks organizations are most concerned about going into 2025:

1. Increase in cybersecurity attacks at vendors
2. Use of artificial intelligence (AI) by our vendors
3. Pending or anticipated regulatory changes
4. Vendors' operational resilience

When asked about the biggest vendor risks organizations are bracing for in the coming year, four key areas emerged:

1. **Increase in cybersecurity attacks at vendors** – A majority of respondents (50%) identified rising cyber threats as their primary concern, making this the dominant risk factor. The escalating frequency and sophistication of vendor-related breaches underscores the urgent need for stronger third-party cyber resilience.

2. **Use of artificial intelligence (AI) by vendors** – With AI adoption accelerating, organizations are worried about how vendors implement AI in their operations. Nearly one-third (30%) of respondents rated this as a significant risk, signaling concerns over bias, regulatory implications, and potential security vulnerabilities in AI-driven vendor services.

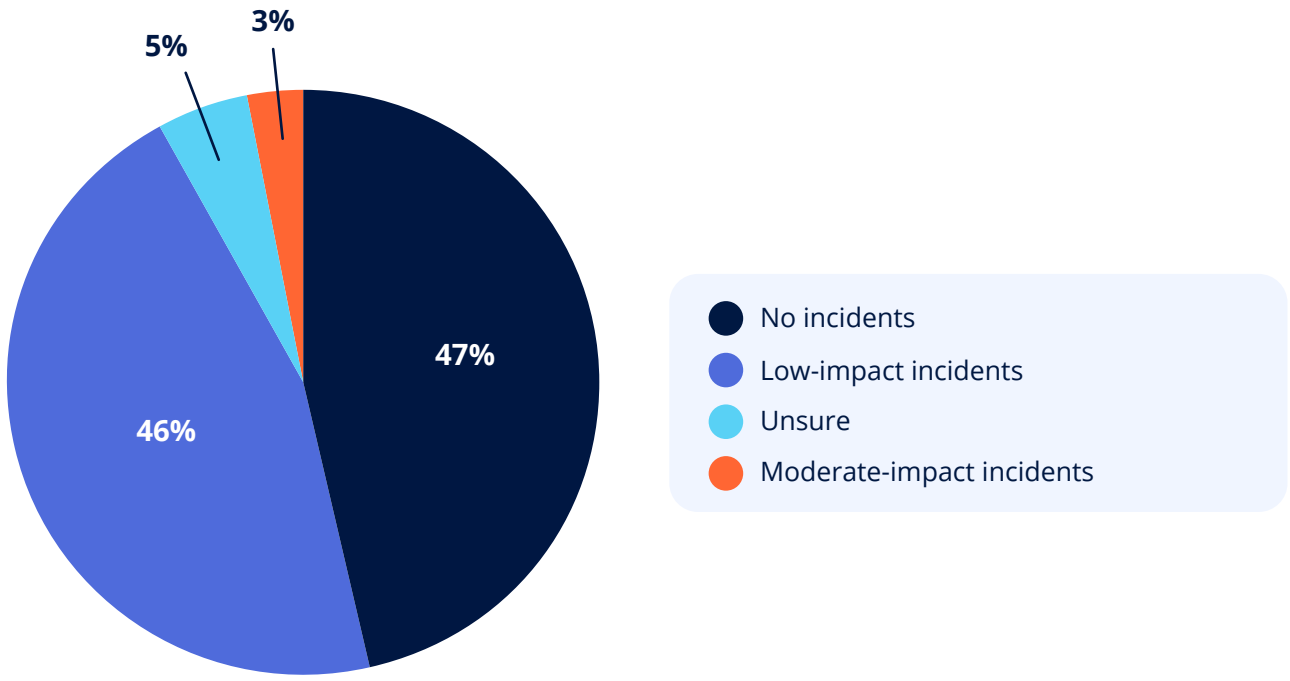
3. **Pending or anticipated regulatory changes** – The uncertainty of evolving regulations is another top concern. Compliance teams face increasing pressure to keep up with new third-party risk management requirements.

4. **Vendors' operational resilience** – Disruptions in vendor operations due to economic shifts, supply chain issues, or systemic risks are a growing concern. Organizations are prioritizing contingency planning to mitigate these risks.

Vendor Cybersecurity Risk & Artificial Intelligence

Avoiding third-party incidents is among the top reasons why financial institutions invest in third-party risk management — a wariness justified by the large number of third-party incidents reported. Nearly half of respondents (49%) reported experiencing a low-impact (limited adverse effects) or moderate-impact (incidents that had significant adverse effects) third-party cyber incident over the past 12 months.

Over the past 12 months, has your organization experienced a third-party cyber incident?



Third-party cyber incidents impacted financial institutions in many ways: reputation damage (28%), financial costs (26%), and regulatory scrutiny (21%). Respondents reported business disruptions, the threat of having to delay loan closings, implementing operational workarounds, civil suits, service delays, and time away from strategic work.

The length of the recovery process varied from institution to institution. While two-thirds (66%) said it took less than 60 days to recover after the incident, 11% said recovery took 60-90 days, and 8% said it took more than 90 days. Another 2% said recovery was still ongoing.

Financial institutions are also concerned about vendor use of artificial intelligence, and the vast majority are currently monitoring vendor AI usage. Just one-third (34%) of institutions under $1B report no current monitoring efforts, compared to 15% of those above $10B.

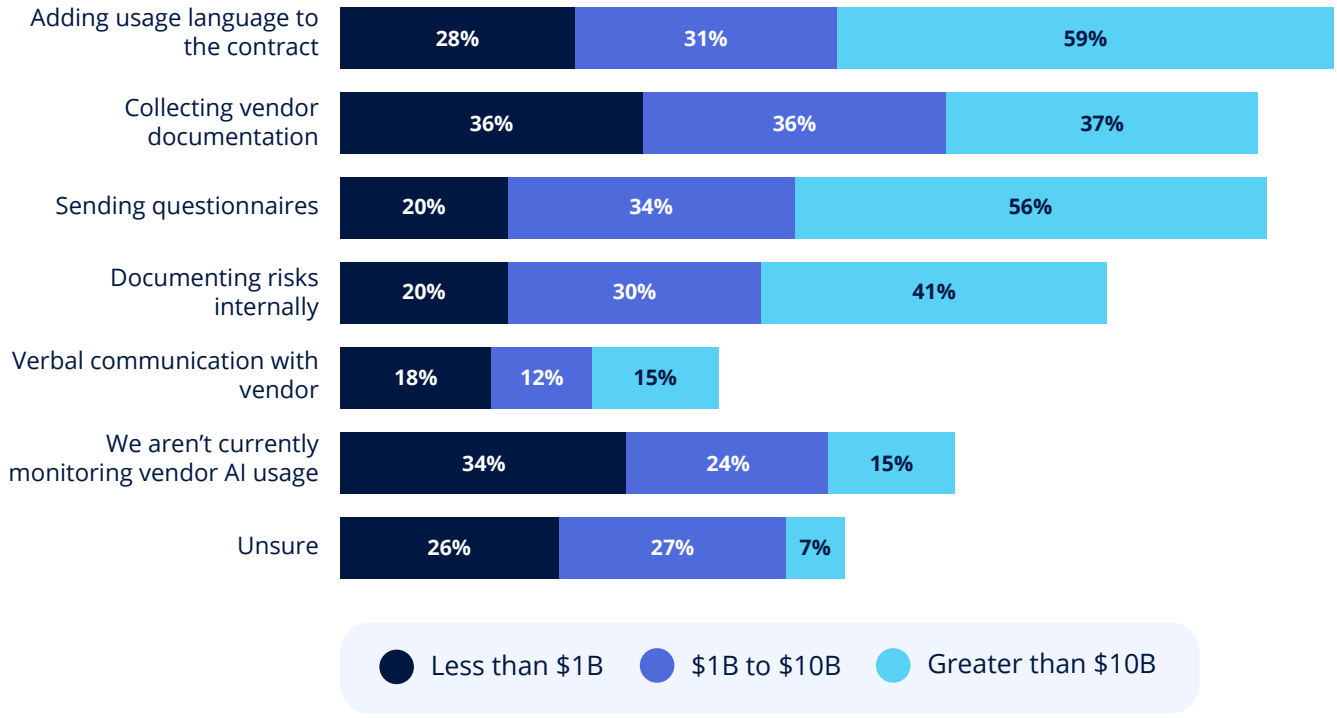
Financial institutions overwhelmingly rely on two key methods for managing AI-related vendor risk: adding AI usage language to contracts and collecting vendor documentation — both of which serve as strong controls to mitigate risk.

According to the data, larger institutions ($10B+) are significantly more proactive in formalizing AI oversight. Nearly 60% incorporate AI-usage terms into contracts, compared to just 28% of institutions under $1B. Similarly, over half (56%) of institutions above $10B send AI-specific questionnaires, while mid-sized and smaller institutions lag behind at 34% and 20%, respectively.

One approach that is notably rare — especially among larger institutions — is relying on verbal assurances from vendors. Just 15% of financial institutions above $10B engage in verbal discussions as a primary method of AI-risk oversight. The reason is clear: vendor promises don't hold weight unless they're in writing.

As AI adoption accelerates, financial institutions of all sizes are likely to adopt more of these controls.

How is your organization currently or planning to assess/monitor vendor usage of artificial intelligence (AI)?



Recommendations and Best Practices

The survey results are clear — financial institutions are under more pressure than ever to refine their third-party risk management (TPRM) programs. Vendor portfolios are growing, cyber risks are escalating, and regulators are paying close attention. To stay ahead, institutions need to modernize their approach, strengthen oversight, and ensure their TPRM programs are both effective and scalable. Here's how to make that happen:

1. **Refine Your TPRM Operating Model for Scalability**
As vendor risk management becomes more complex, relying on a one-size-fits-all approach is no longer sustainable. Many institutions are moving toward a hybrid TPRM model, where a dedicated risk team oversees the framework while vendor owners handle day-to-day monitoring. This structure provides flexibility, consistency, and accountability, ensuring vendor risk management keeps pace with institutional growth. It also helps spread the work when an institution has limited resources.

2. **Align Oversight Frequency with Actual Risk**
Not all vendors pose the same risk, so why treat them the same? High-risk vendors require deeper, more frequent oversight, while lower-risk relationships follow a more streamlined approach. Tying vendor risk assessments to service-specific exposure — rather than broad vendor categories — helps institutions allocate resources efficiently and improve risk mitigation.

3. **Pay Attention to Vendor AI Risk**
AI is an emerging risk that requires attention. Make sure you're integrating AI-specific due diligence into contracts. Taking a proactive stance on risks will protect institutions from financial, operational, and reputational fallout.

4. **Leverage Technology to Manage Vendor Growth**
With financial institutions managing more vendors than ever, relying on spreadsheets and email chains isn't a best practice. The institutions seeing the most success in TPRM are those investing in TPRM software and services that centralize vendor data, automate workflows, improve risk tracking, and simplify due diligence. Not only does this streamline operations, but it also helps institutions demonstrate strong oversight to regulators.

5 **Make TPRM a Competitive Advantage, Not Just a Compliance Obligation**
The institutions leading the way in TPRM aren't just meeting regulatory expectations — they're using vendor risk management as a business differentiator. By strengthening due diligence, refining oversight models, and adopting a proactive, tech-driven approach, financial institutions can reduce costs, improve vendor performance, and strengthen operational resilience.

Next Steps: Is Your TPRM Program Keeping Up?

With heightened regulatory expectations, growing cyber threats, and increasing vendor complexity, now is the time to assess whether your TPRM program is positioned for long-term success. Take stock of your risk assessment processes, technology investments, and oversight strategies to ensure they're evolving with the changing landscape. Institutions that act now will be best positioned to mitigate risk — and stay ahead of the curve.

Strengthen Your Third-Party Risk Management with Ncontracts

Ncontracts is the leading provider of integrated compliance, risk management, and vendor solutions for the financial services industry, serving more than 5,000 organizations worldwide, including 4,000 U.S. financial institutions, mortgage companies, and fintechs.

Focused on simplifying and strengthening all facets of risk management — including TPRM programs — Ncontracts empowers financial institutions with scalable solutions that support growth and program maturity.

Our TPRM Offerings

Nvendor – TPRM Software for Financial Institutions
Simplify vendor management with automated due diligence, contract tracking, risk assessments, and monitoring designed for financial institutions.

TPRM Control Assessments
Comprehensive vendor due diligence providing thorough, risk-based analysis of vendor control environments.

Venminder – TPRM Software for Enterprise & Wealth Management
Manage vendors, track contract data, perform due diligence, assess risks, monitor threats, and more.

Stay Updated on Third-Party Risk Management

Webinars

Nsight Blog

TPRM Certification Training Program

Checklists, Guides & Other Free Resources

Third Party ThinkTank Community

LinkedIn